Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.S1, 2018, pp.87-89
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2018.7.S1.1798

A Survey on Security Models for Data Privacy in Big Data Analytics

Avula Satya Sai Kumar[1], S. Mohan[2] and R. Arunkumar[3]
[1]Research Scholar, [2&3]Assistant Professor,
[1,2&3]Department of Computer Science and Engineering, Annamalai University, Tamil Nadu, India
E-Mail: satya.avula@gmail.com, mohancseau@gmail.com, arunkumar_an@yahoo.com

(Received 30 September 2018; Revised 19 October 2018; Accepted 31 October 2018; Available online 7 November 2018)

***Abstract* - As emerging data world like Google and Wikipedia, volume of the data growing gradually for centralization and provide high availability. The storing and retrieval in large volume of data is specialized with the big data techniques. In addition to the data management, big data techniques should need more concentration on the security aspects and data privacy when the data deals with authorized and confidential. It is to provide secure encryption and access control in centralized data through Attribute Based Encryption (ABE) Algorithm. A set of most descriptive attributes is used as categorize to produce secret private key and performs access control. Several works proposed in existing based on the different access structures of ABE algorithms. Thus the algorithms and the proposed applications are literally surveyed and detailed explained and also discuss the functionalities and performance aspects comparison for desired ABE systems.**

***Keywords:* Attribute Based Encryption, Data Privacy, Access Control**

I. INTRODUCTION

With the rapid development of big data technology and services there has been a surge in single individuals, groups and organizations extent their data storage. The storage strategies are needed to be concentrated periodically and developed as based on the demand. The main aspect should be validated with the security aspects. To provide data privacy and secure access control using cryptographic techniques.

In traditional scheme for security in centralized environment, Public Key Encryption scheme (PKE), both the public key and private keys are generated. The public key is used to encrypt the secret message and the private key is used to decrypt the cipher text to obtain the secret message back. In this technique, sender needs to access the public key first. The worst case in this technique is sharing secrets to a group will make the encryption of same message.

The scheme of secret sharing [1] that explains how to share a secret data among groups or individuals. In this scheme, a secret D is divided into n pieces known as (k, n) threshold scheme) such that knowledge of any n or more pieces can easily regenerate secret D; but information of any k-1 or fewer pieces will create reconstruction infeasible.

A novel cryptographic scheme called Identity-Based Encryption algorithm for communication among users without exchanging the public and private key. In this IBE scheme, encrypted data owner can perform encryption based on receivers unique ID. By these unique ID receiver can decrypt message by using identity as a key. It can reduce the key exposure when exchange of keys.

The fuzzy identity based encryption later known as Attribute Based Encryption scheme. The main thing in ABE can afford minimized effort of large amount user key management. Several developments of ABE techniques have proposed based on the different ABE systems. In order to obtain fine-grained access control over ABE Systems, Key-policy Attribute Based Encryption (KP-ABE) [2] and Cipher text-Policy Attribute Based Encryption (CP-ABE) [3]. After that, several improvements have been made based in the performance and security aspects.

In this paper, we discuss the related works for the implementation of ABE Systems; categories of the ABE based applications and their evolutions and issues.

II. RELATED WORKS

The mainstream features for desired ABE systems, and classifies the schemes into different categories [4]. They provide the high level guidance for the related individual modules and selection options for the ABE systems on demand.

The access control mechanism based on the Cipher text Policy-Attribute Based Encryption technique [5]. It deals with the advancements in this scheme and about the desired applications.

III. CATEGORIES OF DESIRED ABE SYSTEMS

Since the introduction of ABE, several works proposed different applications of ABE as well as different ABE systems. Each scheme will have its own representative expression. For convenience, we define the expression and notation, see below:

Previous IBE system treats identity as a string of characters. The purpose of the Fuzzy Identity-Based Encryption becomes the original ABE system view user's identity as a set of descriptive attribute. In this scheme, cipher text is described with a set of attributes S and a users private key was associate with another set of attributes S and a threshold value k. User can decrypt the message only if at least k attribute are same, which will examined via secret sharing. The structures of original ABE are:

Setup (d): Authority generates public key PK and a master key MK. d is threshold value.
Key-Gen (AU, PK, MK): **A**uthority generates private key D for data users U based on attribute AU.
Encrypt (ACT, PK, M): Data owner encrypts message M with a set of attribute ACT and get cipher text CT.
Decrypt (CT, PK, D): Data user decrypt cipher text CT with private key D if attributes overlap > d.
Original ABE can achieve coarse-grind access control via user's private key and the encrypted data.

To achieve a fine-grained access control, a Key-Policy Attribute-Based Encryption (KP-ABE) scheme [2]. In KP-ABE, cipher texts are labeled with sets of attributes and private keys are associated with a more generalized access control structure. By leverage the Boolean expression such as AND and OR, this scheme can achieve fine-grained access control that only the user have correct access structure can pass through the cipher text to decrypt. KP-ABE change the attribute set that built into user's private key to a more generalized access tree. Access tree uses AND / OR Boolean formula to achieve a fine-grained access control. The structures are:

Setup: Authority publishes public key PK but keep the master key MK.
Key-Gen (AU-KP, PK, MK): Authority generates private key D for data users U at each leaf node based on attribute AU.
Encrypt (ACT, PK, M): Data owner encrypts message M with a set of attribute ACT and get cipher text CT.
Decrypt (CT, D): This algorithm will be executed by a recursive manner. If CT can pass through the access structure in D. then recipient will be able to get the message.

One disadvantage of KP-ABE is that access policy are built into users private key, so data owner who encrypt data have minor control on who can decrypt. Moreover, data owner have to trust the key issues and employ a trusted server to store all the expressive in plaintext. Those sensitive data are potentially vulnerable when stored over Cloud and once trusted server is compromised, the entire expressive are compromised as well.

A novel attribute-based encryption scheme [3], which is called Cipher text-Policy Attribute-Based Encryption (CP-ABE). In this scheme, attributes are associated with keys and access structures are moved from recipient private key into cipher text, so data owner can determines a policy for who can decrypt.

To solve the problem remain in KP-ABE scheme, CP-ABE moved the access structure to cipher text and attribute set stay associated with Key. The structures are:

Setup: Authority generates public key and master key.
Key-Gen (AU, PK, MK): Authority generates private key D for data users U based on attribute AU.
Encrypt (ACT-CP, PK, M): Data owner encrypt the message with the access structure ACT-CP, output is CT.
Decrypt (CT, D): If recipients attribute can pass through access structure embedded in CT. then can proceed to decrypt message.
Delegate (D, AU): The different part from KP-ABE is cipher text-policy ABE are able to delegate new key from users attribute set. It will take users private key D and attributes AU from users attribute set, and generate a new private key D.

With this feature, CP-ABE can gain some flexibility. Both KP-ABE and CP-ABE are monotonic access structures, which means users ability to access the data were based on their attributes and cannot express the negative attribute to exclude certain user from decryption. An attribute-based scheme that allows user to access the data with private key that can be express in any access formula over attributes.

Non-monotonic ABE are constructed based on KP-ABE, the only difference is Non-monotonic ABE introduce NOT formula into expression to exclude unwanted user, as KP-ABE only contain AND and OR Boolean formula. Later proved that expression can also be used in CP-ABE system.

Both KP-ABE and CP-ABE are monotonic access, which means the access structure can only express positive attributes. With only AND / OR in expression, it would certainly limit the structure of the access tree. Non-monotonic ABE introduce the NOT Boolean formula can now exclude the recipient with certain attributes. This scheme proposes the first method that can add negative constraints to describe an unwanted attribute. The structures are:

Setup (d): Authority generates public key and master key and two more computable functions, which will later be used in Encryption. d is used to indicate the number of attribute need to embedded.
Key-Gen (AU-N, PK, MK): Authority generate private key D for data users U based on attribute AU-N, which represent the attribute tree structure with Non-monotonic access.
Encrypt (AN, PK, M): Data owner encrypt the message with the non-monotonic access structure AN, using two computable functions from Setup step then output CT.
Decrypt (CT, D): If recipients attribute can pass through access structure embedded in CT. then can proceed to decrypt message. This scheme seems will bring more powerful representation to ABE system but in reality are hard to achieve. If too many negative attribute are used to describe message, especially when they are not in related to recipients attribute sets, cipher text could have too many attributes to embed, hence increase the encryption overhead.

IV. COMPARISION STUDY

As an encryption system, ABE must meet the requirement of data confidentiality. Since ABE also built-in access control, user authentication and revocation must be satisfied. Additionally, all the ABE system must against collusion attack to prevent user collaborative to access unauthorized information. Based on those precondition, each type of ABE system provide different feature, and those feature forms the characteristic of each system. Following is several functions that made some stand out from others.

1. *Fault Tolerance:* If ABE use a threshold to determine the access right, it can gain the fault tolerance but will sacrifice the preciseness of access control.
2. *Fine-Grained Access Control (AC):* Use the combination of AND OR NOT expression to build an access structure to achieve a fine-grained access control.
3. *Scalability:* User or group can join or leave the system freely without reset or restart entire system.
4. *Key Delegation:* A user is able to delegate the access right or key to other.
5. *Efficient Revocation:* When revocation occurs, avoid the expensive re-encrypt process to achieve efficiency.
6. *Privacy-Preserving:* In multi-auth. scheme, multiple authorities' cooperative and collect users attribute to impersonate him. Not applicable in centralized auth. scheme since centralized auth. must know the entire attributes user owns.
7. *Accountability:* User doesn't have to fully trust Authorities.

V. CONCLUSION

In this paper, the different categories of Attribute Based Encryption scheme and their enhancements are discussed with their pros and cons. using this survey, the future research based in the ABE desired application systems should be chosen through its features as discussed.

REFERENCES

[1] A. Shamir, "How to share a secret", *Communications of the ACM*, Vol. 22, No. 11, pp. 612–613, 1979.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", *In Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM*, pp. 89–98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption", *In Security and Privacy, 2007. SP 07. IEEE Symposium on. IEEE*, pp. 321–334, 2007.

[4] Zhi Qiao, S. Liang, S. Davis and H. Jiang, "Survey of attribute based encryption", *15th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel Distributed Computing*, June, 2014.

[5] G. K. Sandhia and Dr. S. V. Kasmir Raja, "Survey on Attribute Based Encryption schemes for securing the data in cloud environment", *International Journal or Pure and Applied Mathematics*, Vol. 115, No. 6, pp. 565-569, 2017.